U.S.T.A. BRAND PROTECTION AND TAKEDOWN SERVICES

PRODAFT

Protect your brand name, customers and reputation using advanced Brand Protection features of the U.S.T.A. Cyber Threat Intelligence Platform

Phishing Site Detection

Thanks to their easy-to-configure nature, phishing sites have always been a steady trend in cyber fraud. Regardless of their size and location, virtually all banking institutions, cryptocurrency exchange platforms, e-commerce vendors, airline companies, payment gateways and other similar service providers are targeted by cyber fraudsters. Cyber fraudsters target these institutions using phishing websites, impersonating actual websites, brand names and online services.

In terms of detection and takedown of phishing websites, U.S.T.A. has been a trusted partner of hundreds of organizations since 2013.

U.S.T.A.

In the last five years, ***U.S.T.A. has detected more than half a million phishing campaigns*** on behalf of its platform members.

Overcoming Evasion Tactics of Fraudsters with Multiple Detection Channels

Cybercriminals are known for their talent for adaptation. When a new detection method is effective in discovering phishing sites, threat actors come up with new mediums of evasion to hide their phishing websites deeper and extend their lifespan.

For this reason, PRODAFT's R&D team has constantly challenged itself to think one step ahead and design new detection methodologies for future evasion techniques. The U.S.T.A. CTI platform is reinforced with ***six different detection mechanisms*** (based on keyword, structure, image, and other similarities) that monitor the cyber-world to discover phishing websites targeting U.S.T.A. member organizations.

Thanks to this superior detection efficiency, U.S.T.A.'s client turnover is zero. More than 30 large-scale banking institutions have continued to trust U.S.T.A. with their reputation for the last ten years.

Unlimited Takedown, Guaranteed Performance

U.S.T.A. does not require its clients to purchase additional services, tokens or packages when a new phishing attempt is detected. Our experience tells us that; an organization may never know when a phishing trend may turn against them as cyber fraudsters shuffle their targets throughout each year.

When an organization enrolls in the U.S.T.A. platform, they are guaranteed to be kept safe against all potential, expected or active phishing threats. The U.S.T.A. CTI platform ensures the detecting and takedown of all phishing threats without requiring any additional request or interaction. Users of the U.S.T.A. platform may sit back and watch the threats being taken down one after another.

U.S.T.A. →

Despite the contractual 48-hour guarantee, U.S.T.A.'s average takedown time has been ***2 to 4 hours*** in the last two years.

Social Media Detection and Takedown

Social media has become a vital phishing medium for threat actors, especially in the last five years. By impersonating actual organizations via fake social media pages or profiles, threat actors trick unsuspecting customers or organizations into visiting a phishing website or downloading a malicious application.

To cope with this easy-to-perform yet effective attack trend, U.S.T.A. searches Facebook, Twitter and Instagram with multiple techniques and methodologies. Our clients can observe “active” and “potentially suspicious” profiles targeting their organization. Similar to phishing website detection and takedown, all detected active threats are taken down without requiring any request or interaction on the client side.

Decrease the Workload of Your Personnel with Verified Detections

U.S.T.A. →

U.S.T.A. is designed to decrease the workload of its users. Therefore, all findings and detections are verified and classified before being sent to platform users.

This verification is performed using U.S.T.A.’s proprietary A.I. modules and U.S.T.A. operators. Therefore, our clients are not required to go through thousands of potential violations or approve any findings.

Using the intuitive U.S.T.A. user interface, the user can easily filter out all active, potential, and taken-down threats.

In addition to what U.S.T.A. can detect, users of the platform can easily submit their own threats, which U.S.T.A. operators will process for takedown operations in less than minutes.